Atitit 安全技术访问控制 ABAC 与IBAC RBAC

目录

[1. 访问控制的三个基本要素：主体（请求实体）、客体（资源实体）、控制策略（属性集合）； 1](#_Toc21047)

[2. 发展历程 1](#_Toc9473)

[2.1. 示意图： 2](#_Toc13181)

[3. 访问控制理论模型： 2](#_Toc17389)

[3.1. DAC&MAC模型 2](#_Toc11681)

[3.2. IBAC模型：基于身份的访问控制id-Based Access Control 3](#_Toc29545)

[3.3. RBAC模型：基于角色的访问控制（Role-Based Access Control） 3](#_Toc23960)

[3.4. ABAC模型： 3](#_Toc24552)

[3.5. 基于身份的访问控制（IBAC）不 4](#_Toc31760)

[3.6. 基于角色的访问控制（RBAC 4](#_Toc19778)

[4. 他们之间的关系 4](#_Toc31708)

[5. Ref 4](#_Toc4081)

# 访问控制的三个基本要素：主体（请求实体）、客体（资源实体）、控制策略（属性集合）；

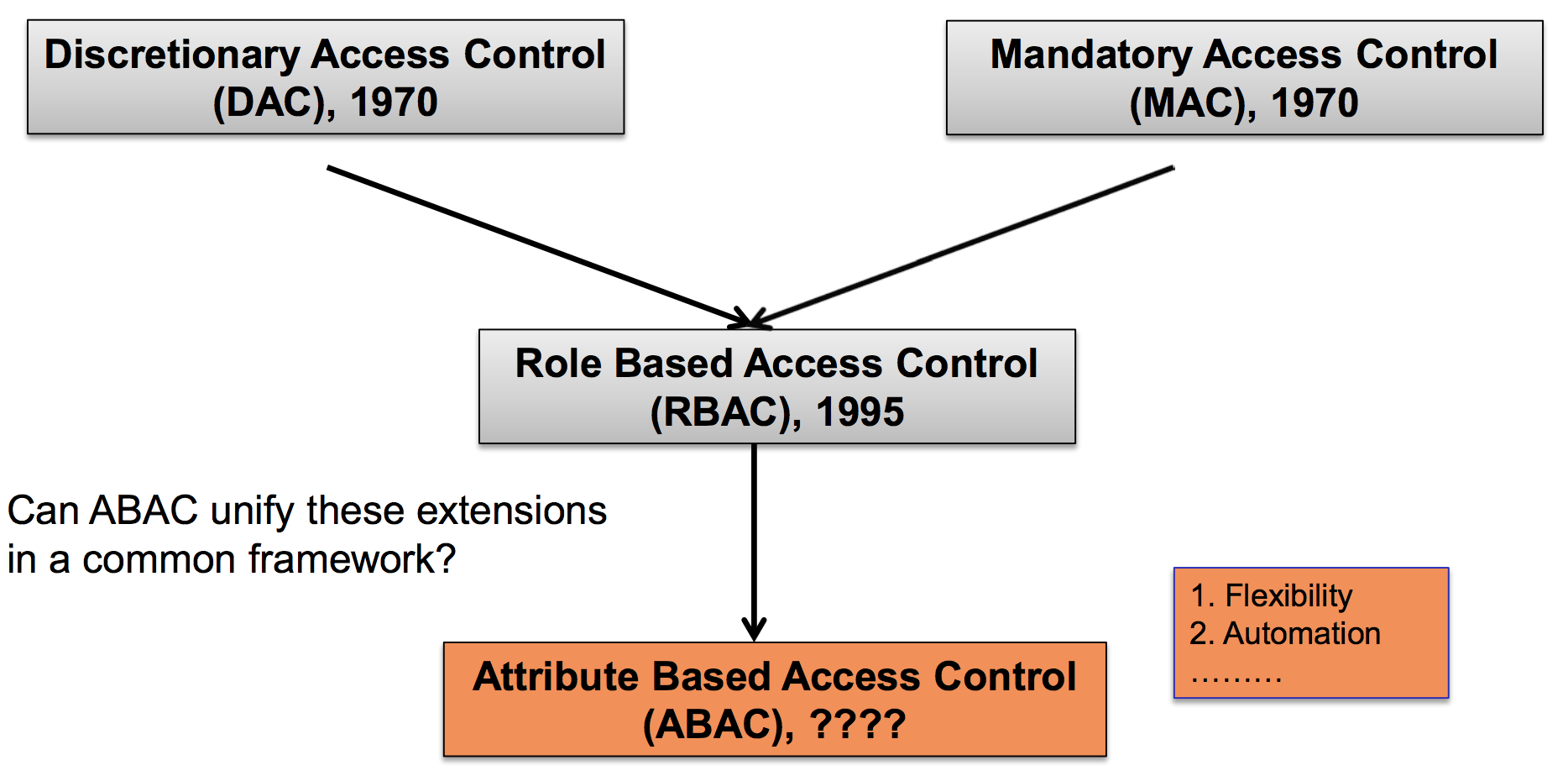
俗的解释就是“【谁】是否有可以对某个【资源】进行某种【操作】”；可以看出访问控制的三个基本要素：主体（请求实体）、客体（资源实体）、控制策略（属性集合）；

# 发展历程

访问控制是信息安全的关键技术之一, 它依赖于其他安全服务并与这些服务共存于信息系统中, 从而提供信息安全保障。

人类使用访问控制技术历史悠久。门锁和钥匙就是一种典型的访问控制。现代访问控制技术起源于20世纪六、七十年代。LAMPSON提出访问控制的形式化和机制描述, 引入了主体、客体和访问矩阵的概念, 它们是访问控制的基本概念[[3](http://netinfo-security.org/article/2016/1671-1122-0-12-19.html" \l "b3-1671-1122-0-12-19)]。从计算技术早期至今, 对访问控制模型的研究大致经历了以下几个阶段：

## ****示意图：****



# ****访问控制理论模型：****

## DAC&MAC模型

* + DAC：自主访问控制；
  + MAC：强制访问控制，一般用于多级安全军事系统；

## IBAC模型：基于身份的访问控制id-Based Access Control

* + 基于身份的访问控制模型
  + 举例：登录验证
  + 比如Java中使用cookie、session存储回话标识；

传统的访问控制以用户为中心, 使用标识符来表示主体。如果主体是人, 其标识符就是身份证号。在RBAC中, 主体则是角色, 而客体、环境和操作等也是角色

## RBAC模型：基于角色的访问控制（Role-Based Access Control）

* + 基于角色的访问控制（Role-Based Access Control）
  + 用户、角色、权限
  + RBAC是ABAC的一种单属性特例；
  + 1992年David F.Ferraiolo & D.Richard Kuhn在第十五届国家计算机安全会议上提出；
  + 论文：<https://csrc.nist.gov/projects/role-based-access-control>
  + 举例：丰趣-小二后台的认证授权模型设计；
  + Spring Security、Apache Shiro、Ali ACL
* RBAC既可实现MAC, 也可实现DAC。从这个意义上说, RBAC是中性的。从控制强度上说, 它属于强制访问控制。RBAC已经得到广泛应用

## ABAC模型：

* + 基于属性的访问控制模型 (Attribute Based Access Control)
  + 举例：阿里云、AWS；

## 基于身份的访问控制（IBAC）不

## 基于角色的访问控制（RBAC

ABAC是一种为解决行业分布式应用可信关系访问控制模型,它利用相关实体(如主体、客体、环境)的属性作为授权的基础来研究如何进行访问控制。基于这样的目的,可将实体的属性分为主体属性、客体属性和环境属性,这与传统的基于身份的访问控制（IBAC）不同。在基于属性的访问控制中，访问判定是基于请求者和资源具有的属性，请求者和资源在ABAC 中通过特性来标识，而不像IBAC 那样只通过ID 来标识，这使得ABAC 具有足够的灵活性和可扩展性，同时使得安全的匿名访问成为可能，这在大型分布式环境下是十分重要的。

# 他们之间的关系

基于角色的访问控制（RBAC）通过引入角色中间元素，使得权限先经过角色进行聚合，然后再将权限分配给主体，通过这种方式可以简化授权，可将角色信息看成是一种属性，这样RBAC 就成为了ABAC 的一种单属性特例

# Ref

系统权限控制体系 \_ 心静志远.html

访问控制技术现状及展望.html

下一代授权模型：基于属性的访问控制 - 安全牛.html